The City of New York

DEPARTMENT OF ENVIRONMENTAL PROTECTION

59-17 Junction Boulevard
Flushing, New York 11373

Emily Lloyd
Commissioner

Joseph F. Singleton, Jr.
Deputy Commissioner

Bureau of Customer Services

April 11, 2007

Office of the Attorney General
State of New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Security Breach at DEP

To Whom it May Concern,

The New York City Department of Environmental Protection ("DEP") discovered during a routine audit of its data searches that one of its employees was performing searches outside of his assigned customer base. This employee was immediately terminated and DEP has been working with its outside vendor to determine the names and addresses of any individual whose information may have been improperly accessed and/or viewed.

DEP has learned that 6 residents of the State of New Hampshire fall into this category and therefore must be contacted.

DEP has mailed all such affected individuals a letter, a sample of which is attached hereto, explaining the details of the security breach and answering any questions thereof.

Please contact me at your earliest convenience if you have any questions or concerns about this situation.

Thank you.

Very truly yours,

Roberto Hernandez
Director of Collections
(718) 595-6689

Cc: A. Rettig, Esq., H. Lam

NOTICE OF DATA BREACH

NYC Department of Environmental Protection • Collections Unit • 59-17 Junction Boulevard, Flushing, NY 11373-5108

March 28, 2007

FIRSTNAME LASTNAME
ADDRESS
CITY, STATE ZIPCODE

Dear FIRSTNAME LASTNAME:

We are writing to you because of a recent data security incident at the NYC Department of Environmental Protection. As we executed our monthly audits on data searches performed by our employees to contact delinquent customers, we found that one of our employees was performing searches outside of the customer base assigned to him. As the first step in our remediation process, we have terminated this individual's employment effective immediately. We also researched every name that was searched by this employee and determined that your information was inappropriately viewed.

To protect you from the possibility of identity theft, the NYC Department of Environmental Protection recommends that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Call any one of the three major credit reporting agencies at a number below to place a fraud alert. Once one agency is notified, then that agency automatically notifies the other two.

You will receive letters from all of them, with instructions on how to get a copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289
http://www.experian.com	http:www.equifax.com	http://www.transunion.com

When you receive your credit reports, please look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Also, look for personal information, such as your home address and Social Security number that may not be accurate. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police precinct or sheriff's office and file a police report of identity theft. Also, get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your credit reports, we recommend that you check your credit report every three months for the next year.

For more information on identity theft, we suggest that you visit the Web site of the NY State Consumer Protection Board (www.consumer.state.ny.us.), or your State or local Consumer Protection Agency.

The NYC Department of Environmental Protection has complied with the New York State Information Security Breach and Notification Act and alerted the New York Attorney General's Office, the New York State Office of Cyber Security and Critical Infrastructure Coordination and the Consumer Protection Board.

If there is anything that the NYC Department of Environmental Protection can do to assist you, please call Harris Lam at (718) 595-5599 or Patrick Hendricks at (718) 595-5582.

DATA BREACH – Questions and Answers

NYC Department of Environmental Protection • Collections Unit • 59-17 Junction Boulevard, Flushing, NY 11373-5108

Incident Questions

1. What happened and how did it happen?

A regular monthly audit determined that a NYC DEP employee was performing data searches outside of normal delinquent customer account analysis. This employee was summarily terminated. Research was performed to determine every name that was inappropriately viewed, and notification letters were sent to all concerned parties.

2. What information was taken?

Our investigation has indicated that only social security numbers may have been inappropriately viewed. We currently **do not** have evidence to indicate that any further improper action was taken regarding your information. Even though we believe this incident is of low risk for identity theft, we felt it was essential to notify you of the incident.

3. What did this employee do with this information?

We are not certain what this employee did with this information, but this employee was terminated immediately. We currently **do not** have evidence to indicate that data has been misused. Even though we believe this incident is of low risk for identity theft, we felt it was essential to notify you of the incident.

4. How many people were affected?

We cannot disclose this information due to its confidentiality.

5. Is my information still at risk?

No. DEP has suspended use of data searches while we change our processes and controls for customer service and delinquent account research to limit this issue to a one-time incident.

6. Apart from the notification letters, what is DEP doing about this?

DEP has suspended use of data searches while we change our processes and controls for customer service and delinquent account research to limit this issue to a one-time incident. DEP has also notified other governmental agencies, as required by the laws of New York State, including the New York State Office of Cyber Security & Critical Infrastructure Coordination, Consumer Protection Board, and Attorney General's Office.

7. What will DEP do to assist us?

DEP has taken the first step by sending you a notification letter. It is in your best interests to obtain a credit report.

8. Does this mean someone stole my personal information?

No. A regular monthly audit determined that a NYC DEP employee was performing data searches outside of normal delinquent customer account analysis. This employee was summarily terminated. We currently do not have evidence to indicate that data has been misused. Even though we believe this incident is of low risk for identity theft, we felt it was essential to notify you of the incident.

Mitigation Questions

1. What should I do?

We currently **do not** have evidence to indicate that data has been misused. However, we recommend that you obtain a credit report from a major credit reporting agency to ensure there has been no fraudulent activity on your accounts. If you suspect that there are actions in the report that you did not initiate, consider placing a fraud alert in your credit file.

2. What is identity theft?

Identity theft occurs when someone uses another person's personal information, such as a person's name or social security number to take on that person's identity in order to commit fraud or other crimes.

3. What is an identity theft report?

An identity theft report is a report filed with a local, state, or federal law enforcement agency, like your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, and the U.S. Postal Inspection Service.

4. What are fraud alerts?

There are two types of fraud alerts: an initial alert, and an extended alert.

- **An initial alert** stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft.

- **An extended alert** stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft **and** you provide the consumer reporting company with an "identity theft report."

5. Who will pay for the cost of the credit reports?

Individuals are entitled to one free credit report per major credit reporting agency (per the Federal FACTA regulations), per year, for a total of three free reports. These reports may be obtained by calling the respective agencies:

- Experian: 888-397-3742

- Equifax: 800-525-6285
- TransUnion: 800-680-7289

If you have already used your free report(s), you may have to pay for another credit report yourself.

Several states give individuals additional opportunities to obtain free credit reports:
California: Confirmed identity theft victims who live in California may obtain one free report each month for the first 12 months upon request. (California Civil Code 1785.15.3)

Colorado, Maine, Maryland, Massachusetts, New Jersey, and Vermont: Individuals may receive one free credit report each year under state law, in addition to the free report provided by Federal FACTA regulations.

Georgia: Individuals may receive two free credit reports each year under state law, in addition to the free report provided by Federal FACTA regulations.

6. What are the first steps I should take if I'm a victim of identity theft?

If you are a victim of identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

- Place a fraud alert on your credit reports, and review your credit reports.
- Close the accounts that you know, or believe, have been tampered with or opened fraudulently.
- File a report with your local police or the police in the community where the identity theft took place. Police reports can help you deal with creditors who need proof of the crime.
- File a complaint with the Federal Trade Commission.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

7. Should I apply for a new Social Security number?

Under certain circumstances, the Social Security Administration may issue you a new Social Security number — at your request — if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new Social Security number may not resolve your identity theft problems, and may actually create new problems. For example, a new Social Security number does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with those from your new Social Security number. Even when the old credit information is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult for you to get credit. And finally, there's no guarantee that a new Social Security number wouldn't also be misused by an identity thief.

8. How do I prove that I'm an identity theft victim?

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing. Be sure to ask the company representative where you should mail your request. Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents. You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

The company can ask you for:

• proof of your identity. This may be a photocopy of a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers, and

• a police report and a completed affidavit, which may be the FTC ID Theft Affidavit or the company's own affidavit.

Resources

Equifax -- 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Federal Trade Commission (FTC): http://www.consumer.gov/idtheft
You can file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Portion of this FAQ contain information from:
- the FTC website on identity theft: http://www.consumer.gov/idtheft
- the Privacy Rights Clearinghouse: http://www.privacyrights.org